

CASE NO.: ARC920000143US2
Serial No.: 09/777,506
August 12, 2004
Page 7

PATENT
Filed: February 5, 2001

Remarks

Reconsideration of the above-captioned application is respectfully requested. Claims 1, 9, 10, and 11 have been rejected as being anticipated by Kanter et al. (USPP US 2003/0223579), and Claims 1 and 9 have also been rejected as being anticipated by Matyas et al. (USPN 5,200,999) despite the admonition of MPEP §706.02 that rejections should be strictly confined to the best available art, and that cumulative rejections should be avoided. Of the remaining claims, Claims 18 and 21 have been rejected as being obvious over Kanter et al. in view of Sklar (1988 publication), and Claims 2-6, 12-15, 18-22, and 25-27 have been rejected as being obvious over Matyas et al. in view of Sklar. Claims 8, 17, and 24 have been rejected as being obvious over Matyas et al. in view of Krol (USPN 4,512,020), while Claims 7, 16, and 23 have been rejected as being obvious over Matyas et al. in view of Crozier et al. (USPN 6,145,111) and Krol.

In addition, the examiner has made certain comments regarding the present priority claim which are underdeveloped. For example, the examiner simply concludes that the claims recite some subject matter that is not present in serial no. 09/379,049, without identifying the allegedly new subject matter to which he refers. Furthermore, even if some claims recite new subject matter, other claims might not, but the examiner does not say one way or the other whether he believes that all claims recite subject matter that was not supported in the parent application or whether only some claims recite new subject matter. In any case, a reader of the present file history must not assume that Applicant acquiesces in anything the examiner has placed on the record thus far regarding priority.

Moreover, the fact that Applicant has focussed its comments below, distinguishing the present claims from the applied references and countering certain rejections must not be construed as acquiescence in other portions of rejections not specifically addressed.

1055-114.AMD

CASE NO.: ARC920000143US2
Serial No.: 09/777,506
August 12, 2004
Page 8

PATENT
Filed: February 5, 2001

To overcome the substantive rejections, Claim 9 has been amended to incorporate the subject matter of now-canceled Claim 13. Claims 1-12 and 14-27 remain pending.

Rejections Under 35 U.S.C. §102

To support an anticipation rejection, every claim element must be taught or inherent in a single prior art reference, Manual of Patent Examining Procedure (MPEP) §2131.

Claims 1, 9, 10, and 11 have been rejected under 35 U.S.C. §102 as being anticipated by Kanter et al., and Claims 1 and 9 have also been rejected as being anticipated by Matyas et al. Turning to the relied-upon portions of Kanter et al. (paragraphs [0067], [0208], and [0038]), Kanter et al. indeed teaches that a generator matrix of an error correction code is used - but not, in contrast to Claim 1, to define plural sets of keys. Instead, as Kanter et al. clearly teaches in both paragraphs [0067] and [0208], a *single public key* of a public key-private key pair is established by the generator matrix. There is simply no mention made in Kanter et al. of plural sets of keys being derived using the matrix, much less how such might be accomplished. The allegation regarding Claim 10 that Kanter et al., paragraph [0208] teaches "each set represents a set of coordinates in a key matrix" is thus mistaken, to the extent the allegation is understood as asserting that Kanter et al. teaches generating plural sets of keys using a matrix. Since all limitations in Claim 1 have neither been taught nor suggested in Kanter et al., the rejections based on this reference are overcome.

With respect to the relied-upon portions of Matyas et al. (col. 88, lines 43-55 and col. 2, lines 50-60), all col. 88, lines 43-55 teach is that for even-numbered generation modes (0 or 2), public key-private key records cfpkr1 and cfpkr2 are generated with lengths s1, s2 that indicate the number of 8-byte blocks. For

1053-114.AMD

CASE NO.: ARC920000143US2
Serial No.: 09/777,506
August 12, 2004
Page 9

PATENT
Filed: February 5, 2001

odd-number generation modes (1), a code-word is used as an input to regenerate cfpkr1 and cfpkr2. The relied-upon portion of column 2 of Matyas et al. is of no further help, merely summarizing the basic Diffie-Hellman concept of public key-private key cryptography.

Accordingly, nothing in Matyas et al. even mentions using "error correction", much less the use of ECC to generate plural sets of keys. The allegation to the contrary in paragraph 12 of the Office Action is simply incorrect - Matyas et al. nowhere even mentions the concept of error correction codes, contrary to what is alleged. The "code word" of Matyas et al., in other words, is just that - it is not the same thing as an error correcting code, just because the word "code" happens to be common to both terms.

Amended independent Claim 9 now sets forth limitations formerly recited in Claim 13, which as admitted by the examiner is taught neither by Kanter et al. nor Matyas et al., overcoming the rejection of Claim 9 under this section.

Rejections Under 35 U.S.C. §103

Claims 18 and 21 have been rejected under 35 U.S.C. §103 as being obvious over Kanter et al. in view of Sklar, and Claims 2-6, 12-15, 18-22, and 25-27 have been rejected as being obvious over Matyas et al. in view of Sklar. Claims 8, 17, and 24 have been rejected under this section as being obvious over Matyas et al. in view of Krol, while Claims 7, 16, and 23 have been rejected as being obvious over Matyas et al. in view of Crozier et al. and Krol.

As set forth above, Kanter et al. fails to teach anything beyond using a generator matrix to establish a single public key of a key pair, and the secondary references nowhere consider cryptography keys at all, but instead are directed to error correction. Accordingly, they cannot supply the teaching missing from

1053-114.AMD

CASE NO.: ARC920000143US2
Serial No.: 09/777,506
August 12, 2004
Page 10

PATENT
Filed: February 5, 2001

Kanter et al. regarding generating plural sets of keys using a matrix. Still less do the relied-upon references teach or suggest, e.g., using a Hamming distance "d" that minimizes key overlap between sets of keys as now set forth in Claim 9, since the only reference that mentions Hamming distance - Sklar - nowhere considers encryption keys, much less the use of a Hamming distance that minimizes overlap between between sets of keys. The rejections under this section based on Kanter et al. have been overcome.

And, since Matyas et al., as shown above, nowhere considers error correcting codes in the context of key generation, the rejections based on a combination of Matyas et al. with the secondary references likewise have been overcome.

In addition, there is no fair *prior art* suggestion to combine Matyas et al. with any of the secondary references, all of which appear to deal with error correcting codes but not encryption keys, because Matyas et al. nowhere considers error correction and the secondary references nowhere consider encryption keys, see MPEP §2143 *et seq.* (more is required in satisfying the MPEP than an observation that the proposed modifications "would have been obvious to one skilled in the art"....rather, in seeking to establish a prima facie case of obviousness, it must be identified where the *prior art* provides a motivating suggestion to make the modifications proposed, *id.*, citing *In re Jones*). Note also that the range of sources available does not diminish the requirement for actual evidence of a prior art suggestion to combine, and "broad conclusory statements regarding the teaching of multiple references, standing alone, are not evidence". *In re Dembiczak*, 175 F.3d 994, 50 U.S.P.Q.2d 1614 (Fed. Cir. 1999).

With respect to the rejections based on Kanter et al. in view of Sklar, Sklar is simply a textbook setting forth details of linear error correction codes, including their generating matrices, but not in any context that would have relevance to Kanter et al. Sklar simply teaches that linear block codes may be used

1053-114.AMD

CASE NO.: ARC920000143US2

Serial No.: 09/777,506

August 12, 2004

Page 11

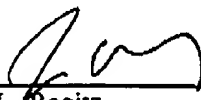
PATENT

Filed: February 5, 2001

to map message vectors into code vectors, but only the present invention has recognized the use of such codes in generating plural sets of encryption keys. Sklar certainly does not even contemplate encryption at all, much less encryption keys, but only error correction. And as set forth above, Kanter et al. nowhere motivates the use of an ECC generating matrix to do anything other than to generate a single public key. Accordingly, even if Sklar were to be combined with Kanter et al., the propriety of which Applicant does not concede, the combination would fail to result in, e.g., Claim 18, which requires defining plural sets of keys using a non-random function based on the number of columns in a key matrix and the number of rows in the key matrix. Instead, Kanter et al. combined with Sklar would result at most in Kanter et al. using an ECC generating matrix of Sklar to generate a single public key of a private key-public key pair, as taught by Kanter et al.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-114.AMD